UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/037,109	10/22/2001	Dany Margalit	U 013682-7	5947

7590 10/19/2005

Ladas & Parry
26 West 61st Street
New York, NY 10023

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 10/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/037,109	MARGALIT ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-88,113-147,172-206 and 231-243* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-88,113-147,172-206 and 231-243* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/12/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication dated 7/25/2005.

Election/Restrictions

This application contains claims directed to the following patentably distinct species of the claimed invention:

I. Claims 89-100, 148-159, and 207-218 are directed towards a server subsystem for detecting malicious content (See Fig. 5A).

II. Claims 101-112, 160-171, and 219-230 are directed towards a client subsystem for detecting malicious content (See Fig. 5B).

III. Claims 113-123, 172-183, and 231-242 are directed towards a gateway subsystem for detecting malicious content (See Fig. 5C).

Applicant's election without traverse of Invention III, which includes claims 113-123, 172-183, and 231-242, in the reply filed on 7/25/2005 is acknowledged.

Claims 1-88, 113-147, 172-206, and 231-243 have been examined.

Title

The title of the invention is acceptable.

Priority

This application has no priority claimed.

Therefore, the effective filing date for the subject matter defined in the pending claims in this application is 10/22/2001.

Information Disclosure Statement

The information disclosure statement(s) (IDS) submitted on 2/12/2002 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statements.

Drawings

The drawings filed on 10/22/2001 are acceptable for examination proceedings.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract of the disclosure is objected to because:

The abstract of the disclosure fails to meet the minimum length requirement of 50 words.

Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the.

invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-14, 17-22, 67-80, and 83-88 are rejected under 35 U.S.C. 102(e) as being anticipated by Le Pennec et al. (US Patent Application Publication 2001/0020272) hereinafter referred to as Le Pennec.

Regarding claim 1, Le Pennec disclosed a method of detecting malicious content comprising: examining at least two characteristics of a digital object (See Le Pennec Paragraph 0192); analyzing said at least two characteristics to determine whether there exists a mismatch therebetween (See Le Pennec Paragraph 0192); and upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content (See Le Pennec Paragraph 0198).

Regarding claim 67, Le Pennec disclosed a system for detecting malicious content comprising: a digital object examiner, examining at least two characteristics of a digital object (See Le Pennec Paragraph 0192); a characteristics mismatch detector, analyzing said at least two characteristics to determine whether there exists a mismatch therebetween (See Pennec Paragraph 0192); and a digital object classifier, operative upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content (See Le Pennec Paragraph 0198).

Regarding claims 2-3, and 68-69, Le Pennec disclosed that malicious content comprises malicious code, and masqueraded content (See Le Pennec Paragraphs 0009-0017).

Regarding claims 4-6, 17-22, 70-72, and 83-88, Le Pennec disclosed that at least one of said at least two characteristics is selected from a set consisting of: header information; file

content; file name extension; and file icon (See Le Pennec Paragraph 0192 wherein the signature of the file was computed which includes all of the listed characteristics of the file).

Regarding claims 7-14, and 73-80, Le Pennec disclosed said digital object is selected from a set consisting of: a file; an e-mail attachment; a web page; and a storage medium (See Le Pennec Paragraph 0023).

Claims 23-36, 39-40, 44, 126-139, 142-143, 147, and 172-184 are rejected under 35 U.S.C. 102(e) as being anticipated by Stewart et al. (US Patent Number 6,901,519) hereinafter referred to as Stewart.

Regarding claims 23 and 126, Stewart disclosed a method of detecting malicious content comprising: obtaining information relating to at least two characteristics of a digital object (See Stewart Col. 3 Line 46 – Col. 4 Line 3); analyzing said information to categorize said digital object into at least two categories (See Stewart Col. 3 Line 46 – Col. 4 Line 3); comparing said at least two categories to decide whether there exists a mismatch therebetween (See Stewart Col. 3 Line 46 – Col. 4 Line 3); upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content (See Stewart Col. 3 Line 46 – Col. 4 Line 3).

Regarding claims 24-25, and 127-128, Stewart disclosed that malicious content comprises malicious code, and masqueraded content (See Stewart Col. 1 Lines 21-39).

Regarding claims 26-28, 39-40, 44, 129-131, 142-143, and 147, Stewart disclosed that at least one of said at least two characteristics is selected from a set consisting of: header information; file content; file name extension; and file icon (See Stewart Col. 3 Line 46 – Col. 4 Line 3 wherein the extension is header information).

Regarding claims 29-36, and 132-139, Stewart disclosed that said digital object is selected from a set consisting of: a file; an e-mail attachment; a web page; and a storage medium (See Stewart Col. 3 Lines 56-58).

Regarding claims 172-184, Stewart disclosed that said digital object information obtainer comprises a digital object information obtainer gateway subsystem; said characteristic based categorizer comprises a characteristic based categorizer gateway subsystem; said categories mismatch detector comprising a mismatch detector gateway subsystem; and said digital object classifier comprising a mismatch detector gateway subsystem (See Stewart Fig. 1 Element 102 and Col. 3 Lines 28-45).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 15-16, 45-66, 81-82, and 185-206 are rejected under 35 U.S.C. 103(a) as being unpatentable over Le Pennec.

Regarding claims 45 and 185, Le Pennec disclosed examining at least two characteristics of a digital object; analyzing said at least two characteristics to determine whether there exists a mismatch therebetween; and upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content (See the rejection of

claim 1 above), but failed to disclose that the characteristics may be selected by the creator of the digital object independently of selection of another characteristic and further failed to disclose that the object could be a web page or storage medium.

It was well known in the art at the time of invention that the creator of a digital signature could select what was being signed. Furthermore, it was well known in the art that web pages and storage mediums could contain malicious content and as a result should be checked for malicious content. It therefore would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was known in the art in the signature system of Le Pennec by allowing the creator of the file to sign whichever portions of the file the creator chose. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a more flexible environment for the creator. It further would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was known in the art in the signature system of Le Pennec by applying the signature checking to web sites and storage mediums as well. This would have been obvious because the ordinary person would have been motivated to protect against malicious content in web pages and storage mediums as well as files and attachments.

Regarding claims 46-58, 61-66, 186-198, and 201-206, see the rejections of claims 2-14, and 17-22 above.

Claims 113-125, and 231-243 are rejected under 35 U.S.C. 103(a) as being unpatentable over Le Pennec as applied to claims 67 and 185 above, and further in view of Touboul et al. (US Patent Number 6,154,844) hereinafter referred to as Touboul.

Le Pennec disclosed a system for detecting malicious content comprising: a digital object examiner, examining at least two characteristics of a digital object (See Le Pennec Paragraph 0192); a characteristics mismatch detector, analyzing said at least two characteristics to determine whether there exists a mismatch therebetween (See Pennec Paragraph 0192); and a digital object classifier, operative upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content (See Le Pennec Paragraph 0198), but failed to disclose the system being implemented in a gateway.

Touboul teaches that in order to protect a network, protection such as determining suspicion of downloadable content should be applied in a gateway (See Touboul Col. 5 Lines 13-33).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Touboul in the virus protection system of Le Pennec by applying the protection in a gateway. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the network from transmitting malicious content.

Claims 37-38, and 140-141 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart.

Stewart disclosed a method of detecting malicious content comprising: obtaining information relating to at least two characteristics of a digital object (See Stewart Col. 3 Line 46 – Col. 4 Line 3); analyzing said information to categorize said digital object into at least two categories (See Stewart Col. 3 Line 46 – Col. 4 Line 3); comparing said at least two categories to decide whether there exists a mismatch therebetween (See Stewart Col. 3 Line 46 – Col. 4 Line

3); upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content (See Stewart Col. 3 Line 46 – Col. 4 Line 3), but failed to disclose that the object could be a web page or storage medium.

It was well known in the art that web pages and storage mediums could contain malicious content and as a result should be checked for malicious content.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was known in the art in the virus detection system of Stewart by applying virus detection to web pages and storage mediums as well. This would have been obvious because the ordinary person would have been motivated to protect against malicious content in web pages and storage mediums as well as files and attachments.

Claims 41-43, and 144-146 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart as applied to claims 23, and 126 above, and further in view of Pasawicz ("The Importance of File Extensions").

Stewart disclosed a method of detecting malicious content comprising: obtaining information relating to at least two characteristics of a digital object (See Stewart Col. 3 Line 46 – Col. 4 Line 3); analyzing said information to categorize said digital object into at least two categories (See Stewart Col. 3 Line 46 – Col. 4 Line 3); comparing said at least two categories to decide whether there exists a mismatch therebetween (See Stewart Col. 3 Line 46 – Col. 4 Line 3); upon determination of the existence of a mismatch, classifying said digital object as a digital object possibly containing malicious content (See Stewart Col. 3 Line 46 – Col. 4 Line 3), but failed to disclose checking the icon of the object as well in order to determine suspiciousness of the object.

Pasawicz teaches that there are many telltale signs of malicious files including icon "faking" in which the icon does not match the file type in order to mislead a user into thinking the file is one type (i.e. an image file) when it is actually a different type (i.e. an executable file) (See Pasawicz Page 5 Col. 1).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Pasawicz in the virus detection system of Stewart by checking the icon type in addition to the extension and content types for coincidence. This would have been obvious because the ordinary person skilled in the art would have been motivated to apply the know signs of a malicious file to the detection system in order to trap the most "viruses" as possible.

Conclusion

Claims 1-88, 113-147, 172-206, and 231-243 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Rosenthal (US Patent Number 5,359,659) disclosed determining suspicious files based on the filename vs. file extension.

b. Houser et al. (US Patent Number 5,606,609) disclosed determining suspicious files based on the icon vs. the content.

c. Chen et al. (US Patent Number 5,951,698) disclosed determining suspicious filed based on the extension and the content.

d. Bates et al. (US Patent Number 6,721,721) disclosed checking web pages for viruses.

e. Tsai (US Patent Application Publication 2003/0097409) disclosed parsing an E-mail header and attachments for suspicious content.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

Matthew Henning
Assistant Examiner
Art Unit 2131
10/17/2005